UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

JESSE JAMES PAGAN and LILYANN DAVILA, *on behalf of themselves and all similarly situated persons*,	:	
Plaintiffs	:	
v.	:	Civil Action No. 3:22-cv-297
FANEUIL, INC.,	:	
Defendant.	:	

CLASS ACTION COMPLAINT

Plaintiffs Jesse James Pagan and Lilyann Davila ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint (the "Action") against Faneuil, Inc. ("Defendant" or "Faneuil"), a Virginia-based corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This Action arises out of the recent ransomware attack and data breach at Faneuil that targeted the information of past and present employees who worked at Faneuil (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive data of past and present employees that worked at Faneuil. Because of the Data Breach, thousands of Class Members' suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs and Class

Members are now faced with the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their names, addresses at the time of employment, Social Security numbers, phone numbers, and email addresses (hereinafter, the "Personally Identifiable Information" or "PII").

3. Even worse, after discovering the Data Breach, Faneuil sat on the information for nearly half a year – failing to disseminate data breach consumer notifications until February 1, 2022. When a data set that is inclusive of the aforementioned PII is breached, every moment is precious to ensure that that data is not then weaponized against the rightful owner of that data through identity theft. Sitting on this information allowed Faneuil to dodge responsibility and inevitably worsened the Data Breach victims' chances at weathering the storm that Faneuil created.

4. As a result of the Data Breach, Plaintiffs and Class Members have been harmed – they have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and forever closely monitor their financial accounts to guard against identity theft.

5. Plaintiffs and Class Members may also incur out-of-pocket costs, for example, through having to purchase credit monitoring systems, credit freezes, or other protective measures to deter and detect identity theft. Plaintiffs seek to remedy those harms on behalf of themselves and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

6. As such, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, asserting claims for negligence and breach of implied contract.

II. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act because (1) there are more than 100 putative Class Members, (2) the aggregate amount-in-controversy, exclusive of costs and interest, exceeds $5,000,000.00, and (3) there is minimal diversity because Plaintiffs and Defendant are citizens of different states – namely, that Plaintiffs are Florida residents and the Defendant is headquartered here, in Virginia.

8. This Court has personal jurisdiction over the Defendant because the Defendant is headquartered in this District. Additionally, this Court has personal jurisdiction over the Defendant because they have substantial contacts with this District and have purposely availed themselves to the Courts in this District.

9. In accordance with 28 U.S.C. 1391, venue is proper in this District because a substantial part of the conduct giving rise to the Plaintiffs' claims occurred in this District, the Defendant is headquartered in this District, and the Defendant transacts business within this District.

III. PARTIES

10. Plaintiff Jesse James Pagan. Plaintiff Pagan is a resident and citizen of the state of Florida and was notified of the Data Breach and his PII being compromised by way of a data breach notification letter disseminated by Defendant on or about February 1, 2022.

11. Plaintiff Lilyann Davila. Plaintiff Davila is a resident and citizen of the state of Florida and was notified of the Data Breach and her PII being compromised by way of a data breach notification letter disseminated by Defendant on or about February 1, 2022.

12. **Defendant Faneuil, Inc**.. Defendant Faneuil, Inc. is a logistics and business solutions company based in Hampton, Virginia.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

13. According to Defendant, "Faneuil provides a broad array of business process outsourcing solutions . . . and currently employs more than 5,500 professionals nationwide."[1]

14. According to Defendant's Data Breach Notification letter, with respect to data privacy, "we value the trust that individuals place in us with their information and we understand the importance of protecting the information that we maintain."

15. On information and belief, in the course of collecting PII from consumers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for customer data through their applicable privacy policy and through other disclosures.

16. By obtaining, collecting, using and deriving benefits from Plaintiffs and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

17. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on this sophisticated company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

18. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

---

[1] https://www.faneuil.com/about-us/ (last accessed Apr. 14, 2022).

THE DATA BREACH

19. In February 2022, Defendant first began notifying Class Members and state AGs about a widespread data breach of its computer systems involving the sensitive PII of consumers. According to Defendant, the breach occurred in August of 2021.

20. According to Faneuil's Data Breach Notification, a ransomware attack was discovered on August 18, 2021.[2]

21. Following the incident, Defendant conducted a review of its files and ultimately determined that there had been a data breach involving Plaintiffs' and Class Members' PII.

22. Defendant's investigation and notification letter confirmed the worst: "the attackers accessed and copied certain company records, including records of past and present Faneuil employees." According to Defendant, the PII accessed and stolen in the Data Breach included names, addresses at the time of employment, Social Security numbers (the holy grail for identity thieves), and email addresses.

23. Even worse, rather than promptly informing Class Members about the Data Breach so they could take measures to protect themselves, Defendant opted not to inform consumers until *nearly six months* after the discovery of the Data Breach on February 1, 2022.

---

[2] Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. While at one time the prime motive of a ransomware attack was simply to encrypt a user's data and hold it for ransom, ransomware attacks are now primarily the last phase of a multi-pronged cyberattack that is targeted at confidential data, and that has as its prime motivation the theft of confidential data like the PII stolen here. A recent analysis shows that data exfiltration occurs in 70 percent of all ransomware attacks. Jessica Davis, *70% Ransomware Attacks Cause Data Exfiltration; Phishing Top Entry Point*, HealthITSecurity (Feb. 3, 2021), *available at*: https://healthitsecurity.com/news/70-ransomware-attacks-cause-data-exfiltration-phishing-top-entry-point (last accessed Apr. 20, 2022).

24. The Data Breach resulted in unauthorized access to the sensitive data of current and former Faneuil employees. Because of the Data Breach, thousands of Class Members' suffered ascertainable losses including out-of-pocket expenses and the value of their time incurred to mitigate the effects of the attack and the present and imminent harm caused by the compromise of their sensitive personal information.

25. The Personally Identifiable Information contained in the files accessed in the Data Breach was not encrypted.[3]

26. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to implement and utilize adequate data security measures to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

27. Therefore, the increase in such attacks, and the attendant risk of future attacks was widely known to the public and to anyone in the Defendant's industry, including the Defendant itself.

DEFENDANT FAILS TO FOLLOW FTC GUIDELINES

28. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses to highlight the importance of implementing reasonable data security practices.

[3] It is clear that the information exposed in the Data Breach was unencrypted: California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on or about Feb. 1, 2022, evidencing that the exposed data was unencrypted. *See* https://oag.ca.gov/ecrime/databreach/reports/sb24-550731 (last accessed Apr. 20, 2022).

According to the FTC, the need for data security should be factored into all business decision-making.

29. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[4] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[5]

30. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

31. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[4] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016); *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 20, 2022).
[5] *Id.*

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

32. Defendant failed to properly implement basic data security practices.

33. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

34. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

35. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

36. Other best cybersecurity practices that are standard in the Defendant's industry, and that upon information and belief Defendant did not employ, include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

37. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

38. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S BREACH

39. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

40. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its IT systems which contained unsecured and unencrypted PII.

41. Accordingly, as outlined below, Plaintiffs and Class Members now face present and an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

HARM TO CONSUMERS

42. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

43. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at a present and an increased risk of fraud and identity theft for many years into the future.

44. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

45. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the

suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

46. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[6]

47. The fraudulent activity resulting from the Data Breach may not come to light for years.

48. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

49. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

50. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[6] Brian Naylor, "*Victims of Social Security Number Theft Find It's Hard to Bounce Back*," NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about- identity-theft (last accessed Apr. 20, 2022).

HARM TO PLAINTIFFS

A. HARM TO PLAINTIFF PAGAN

51. Before the Data Breach, Mr. Pagan provided his PII to Faneuil as a requirement for employment with the company. Mr. Pagan would have never provided his PII to Faneuil had he known it lacked adequate data security.

52. In February, 2022, Mr. Pagan received a Notice of Data Breach letter from Faneuil informing him that his full name and Social Security number, amongst other information, was stolen by cyberthieves in the Data Breach. As a result of the Data Breach, Faneuil directed Plaintiff Pagan to take certain steps to protect his PII and otherwise mitigate his damages.

53. As a result of the Data Breach and the directives that he received in the Notice Letter, Mr. Pagan has spent significant time and resources dealing with the Data Breach and continues to this day spending time dealing with the consequences of the Data Breach, including, but not limited to, self-monitoring his bank and credit card accounts, verifying the legitimacy of the *Notice of Data Breach*, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

54. Mr. Pagan is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

55. Mr. Pagan stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

56. Mr. Pagan suffered actual injury and damages due to Faneuil's inadequate measures to safeguard his PII before the Data Breach.

57. Mr. Pagan suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Faneuil for the purpose of providing employment, which was compromised in and as a result of the Data Breach.

58. Mr. Pagan suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

59. Mr. Pagan has suffered present, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and criminals.

60. Mr. Pagan has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Faneuil's possession, is protected and safeguarded from future breaches.

B. HARM TO PLAINTIFF DAVILA

61. Before the Data Breach, Ms. Davila provided her PII to Faneuil as a requirement for employment with the company. Ms. Davila would have never provided her PII to Faneuil had she known it lacked adequate data security.

62. In February, 2022, Ms. Davila received Notice of Data Breach Letter from Faneuil informing her that her full name and Social Security number, amongst other information, was stolen by cyberthieves in the Data Breach. As a result of the Data Breach, Faneuil directed Plaintiff Davila to take certain steps to protect her PII and otherwise mitigate her damages.

63. As a result of the Data Breach and the directives that she received in the Notice Letter, Ms. Davila has spent significant time and resources dealing with the Data Breach and continues to this day spending time dealing with the consequences of the Data Breach, including, but not limited to, self-monitoring her bank and credit card accounts, verifying the legitimacy of the *Notice of Data Breach*, communicating with her bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

64. Ms. Davila is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

65. Ms. Davila stores any and all documents containing PII in a secure location, and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

66. Ms. Davila suffered actual injury and damages due to Faneuil's mismanagement of her PII before the Data Breach.

67. Ms. Davila suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Faneuil for the purpose of providing her employment, which was compromised in and as a result of the Data Breach.

68. Ms. Davila suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

69. Ms. Davila has suffered present, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII,

especially her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

70. Ms. Davila has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Faneuil's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

71. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Personally Identifiable Information was maintained on Faneuil's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class").

72. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

73. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of over 100 individuals whose sensitive data was compromised in the Data Breach.

74. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Personally Identifiable Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

e. Whether Defendant owed a duty to Class Members to safeguard their Personally Identifiable Information;

f. Whether Defendant breached a duty to Class Members to safeguard their Personally Identifiable Information;

g. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

h. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether the Plaintiffs and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

75. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

76. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

77. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

78. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

79. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

NEGLIGENCE
(On behalf of Plaintiffs and the Class)

80. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully alleged herein.

81. Faneuil required Plaintiffs and Class Members to submit non-public Personally Identifiable Information, including but not limited to, Social Security Numbers, as a condition of employment at Faneuil.

82. By collecting and storing this data, and sharing it and using it for commercial gain, Faneuil had and/or voluntarily undertook a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft.

83. Faneuil's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

84. Faneuil also owed a duty of care to Plaintiffs and members of the Class to provide security consistent with industry standards, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' information.

85. Only Faneuil was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Class from a data breach. Faneuil breached

its duty by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personally Identifiable Information.

86. The specific negligent acts and omissions committed by Faneuil include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Personally Identifiable Information;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiffs' and Class Members' Personally Identifiable Information; and

d. failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personally Identifiable Information had been compromised.

87. It was foreseeable that Faneuil's failure to use reasonable measures to protect and monitor the security of Personally Identifiable Information would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Class were reasonably foreseeable.

88. It was therefore foreseeable that the failure to adequately safeguard Personally Identifiable Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent

initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

89. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an order declaring that Faneuil's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

90. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully alleged herein.

91. When Plaintiffs and Class Members provided their Personally Identifiable Information to Faneuil in exchange for employment, they entered into implied contracts with Faneuil pursuant to which Faneuil agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

92. Faneuil solicited and invited prospective and current employees to provide their PII as part of its regular business practices. These individuals accepted Faneuil's offers and provided their Information to Faneuil. In entering into such implied contracts, Plaintiffs and the Class reasonably presumed that Faneuil's data security practices and policies were reasonable and consistent with industry standards, and that Faneuil would use part of the funds received from Plaintiffs' and the Class's labor to pay for adequate and reasonable data security practices.

93. Plaintiffs and the Class would not have provided and entrusted their Information to Faneuil in the absence of the implied contract between them and Faneuil to keep the information secure.

94. Plaintiffs and the Class fully performed their obligations under the implied contracts with Faneuil.

95. Faneuil breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of a data breach.

96. As a direct and proximate result of Faneuil's breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

THIRD CAUSE OF ACTION

Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

98. Plaintiffs re-allege and incorporate by reference paragraphs 1-80 above as if fully set forth herein.

99. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of labor services.

100. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by them.

101. The money that Defendant received from Plaintiffs' and Class Members' labor services should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

102. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

103. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' PII.

104. Under principles of equity and good conscience, Defendant should not be permitted to retain the money it received from Plaintiffs' and Class Members' labor services that should have been used to implement the data security measures necessary to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

105. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiffs' and Class Members' PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

VII. PRAYER FOR RELIEF

97. WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with

the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

E. Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiffs and the Class;

F. For an award of actual damages and compensatory damages, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

VIII. JURY TRIAL DEMAND

Jury trial is demanded by Plaintiffs and members of the putative Class.

DATED: April 26, 2022

Respectfully submitted,

By: /s/ Lee A. Floyd

Lee A. Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
7130 Glen Forest Drive, Suite 400
Richmond, Virginia 23226
Telephone: (757) 622-6000
Facsimile: (757) 670-3939
Lee@bbtrial.com
Justin@bbtrial.com

Jeffrey A. Breit, VSB #18876
Kevin Biniazan, VSB #92019
BREIT BINIAZAN, P.C.
Towne Pavilion Center II
600 22nd Street, Suite 402
Virginia Beach, Virginia 23451
Telephone: (757) 622-6000

Facsimile: (757) 670-3939
Jeffrey@bbtrial.com
Kevin@bbtrial.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

M. Anderson Berry*
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

**pro hac vice forthcoming*